ІНДЕКС ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ 2021

Дослідження корпоративної політики 20 провідних технологічних компаній в Україні на предмет дотримання ними цифрових прав людини в аспекті захисту персональних даних

Загальна редакція:
Віталій Мороз

Експерти дослідження:
Тетяна Авдєєва
Павло Бєлоусов
Лідія Волкова
Віталій Мороз
Аліна Правдиченко

Менеджерка проєкту:
Юлія Бабко

Дизайн та верстка:
Карина Строкань
Денис Балуба

Редакторка:
Юлія Мороз

Експертне дослідження підготувала ГО «Інтерньюз-Україна» за підтримки Європейського Союзу та Міжнародного фонду «Відродження» в межах грантового компоненту проєкту EU4USociety. Матеріал відображає позицію авторів і не обов'язково відображає позицію Міжнародного фонду «Відродження» та Європейського Союзу.

Європейський Союз складається з 27 держав-членів та їхніх народів. Це унікальне політичне та економічне партнерство, основане на цінностях поваги до людської гідності, свободи, рівності, верховенства права і прав людини. Понад п'ятдесят років знадобилось для створення зони миру, демократії, стабільності та процвітання на нашому континенті. Водночас нам удалося зберегти культурне розмаїття, толерантність і свободу особистості. ЄС налаштований поділитися своїми цінностями та досягненнями з країнами — сусідами ЄС, їхніми народами та з народами з-поза їхніх меж.

Міжнародний фонд «Відродження» — одна з найбільших благодійних фундацій в Україні, що з 1990 року допомагає розвивати в Україні відкрите суспільство на основі демократичних цінностей. За час своєї діяльності Фонд підтримав близько 20 тисяч проєктів, до реалізації яких долучилися понад 60 тисяч активістів та організацій України на суму понад 200 мільйонів доларів США. Сайт: www.irf.ua. Facebook: www.fb.com/irf.ukraine

Громадська організація «Інтерньюз-Україна» — організація з досвідом на ринку медіа, комунікацій, освіти та консалтингу з 1996 року.
Сайт: www.internews.ua/. Facebook: www.fb.com/internewsukraine/

ЗМІСТ

ВСТУП

ВСТУП

Стрімкий розвиток цифрових технологій розширює поле правових відносин людей в онлайн-просторі як у світі, так і в Україні. До формування цих відносин в інтернеті залучені також представники приватного сектору та урядові інституції. Однією з тенденцій останнього десятиліття є активні впливи урядів на функціонування онлайн-простору. Нерідко урядові наміри регулювати відносини в онлайн-просторі викликають критику в представників громадянського суспільства та приватного сектору з огляду на ризики для вільного розвитку інтернету.

Однак є й інша сторона регулювання. Унормовування відносин між усіма «гравцями» в національному законодавстві повинно **передбачити реалізацію принципу захисту прав людини в онлайн-просторі**. Це стосується, зокрема, сфери приватності та захисту персональних даних: у цифровій ері обсяг даних і розширення інструментів взаємодій невпинно зростає.

Методи збору та зберігання приватної інформації зазнали суттєвих змін і різняться навіть поміж окремих компаній та організацій, які накопичують та управляють даними мільйонів користувачів. Українські користувачі взаємодіють за посередництва значної кількості інтернет-технологій та отримують послуги в онлайні як від держави, так і від приватного сектору.

Водночас багато користувачів дають згоду на політику збереження та розпорядження їхніми персональними даними, особливо не проблематизуючи цих питань. Реалізуючи дослідження Індекс захисту персональних даних, команда проєкту порушує **питання цифрових прав з позиції «обізнаного користувача».** Чи створюють приватні компанії умови для кращого розуміння користувачами своїх прав в онлайн-просторі? Чи передбачили приватні компанії у функціоналі своїх сервісів усвідомлену згоду користувача на опрацювання їхніх персональних даних? Чи відповідає корпоративна політика приватних компаній міжнародним стандартам захисту прав людини та українському законодавству у сфері персональних даних?

Згідно з чинним українським законодавством, приватні компанії у взаємодії з користувачами зобов'язані дотримуватися **Закону «Про захист персональних даних».** Закон ухвалили 2011 року, у час, коли увага до онлайн-простору ще не була визначальною, а інтенсивність взаємодій користувачів була нижчою, ніж сьогодні. Водночас Україна стоїть на порозі **ухвалення нової законодавчої ініціативи, що регулюватиме захист персональних даних.** 7 червня 2021 року законопроєкт № 5628 про захист персональних даних внесли в порядок денний Верховної Ради України. Цей законопроєкт містить значну частину положень, які впровадять ефективні механізми захисту персональних даних користувачів та гармонізують національне законодавство з підходами Європейського Союзу щодо захисту персональних даних — такими є ключові результати дослідження законопроєкту № 5628 від ГО «Інтерньюз-Україна» в межах Індексу регулювання онлайн-простору, представлені в серпні 2021 року. Зведена оцінка дослідження законопроєкту № 5628 становила +0,87 у межах шкали від –5 до +5.

Утім, законодавчі зміни не завжди гарантують зміни інституційної поведінки, і положення національного законодавства не завжди відображають усі нюанси міжнародних стандартів прав людини. Саме тому зусилля щодо впровадження розуміння цифрових прав людини й розширення спектру їхнього застосування реалізуються і в проєктах громадських організацій в Україні.

Індекс захисту персональних даних — імовірно, перше в Україні дослідження, що **виносить на широку дискусію питання щодо політики та практики поваги до персональних даних українських користувачів з боку приватного сектору.** Це дослідження дасть змогу окреслити ключові виклики щодо захисту персональних даних користувачів, на які приватні компанії здатні дати відповіді вже найближчими місяцями. Ми віримо, що **культивування поваги до персональних даних на рівні корпоративної політики є глобальним трендом представників відповідального бізнесу, до якого здатні долучитися й приватні компанії, що працюють в Україні.**

Під час першого дослідження, проведеного 2021 року в контексті захисту цифрових прав користувачів, **команда проєкту дослідила сайти 20 великих приватних компаній в Україні** у сфері телекомунікацій, надання послуг доступу до інтернету та онлайн-сервіси. До списку ввійшли такі компанії / бренди:

ПрАТ «Київстар» — Kyivstar.ua

ТОВ «Лайфселл» — Lifecell.ua

ПрАТ «ВФ Україна» — Vodafone.ua

ПРАТ «ДАТАГРУП» — DataGroup.ua

ТОВ «ТРІОЛАН» — Triolan.com

ТОВ «РОЗЕТКА.УА» — Rozetka.com.ua

ТОВ «УАПРОМ» — Prom.ua

ТОВ «ЄМАРКЕТ УКРАЇНА» / OLX Global BV — Olx.ua

Український інтернет-холдинг ТОВ «Укрнет» — Ukr.net

ТОВ «Нова Пошта» — NovaPoshta.ua

ТОВ «КОМФІ ТРЕЙД» — Comfy.ua

ТОВ «ГК "ФОКСТРОТ"» — Foxtrot.ua

ТОВ «ІД ЕЛЬДОРАДО» — Eldorado.ua

ТОВ «ЗТ-ІНВЕСТ» — Citrus.ua

ТОВ «АЛЛО» — Allo.ua

MAKEUP GLOBAL/ТОВ «Мейкап» — Makeup.com.ua

ТОВ «КАСТА ГРУП» — Kasta.ua

ТОВ «СІЛЬПО-ФУД» — Silpo.ua

ТОВ «Заказ Юкрейн» — Zakaz.ua

ТОВ «ЛАНЕТ ТЕЛЕКОМ» — Lanet.ua

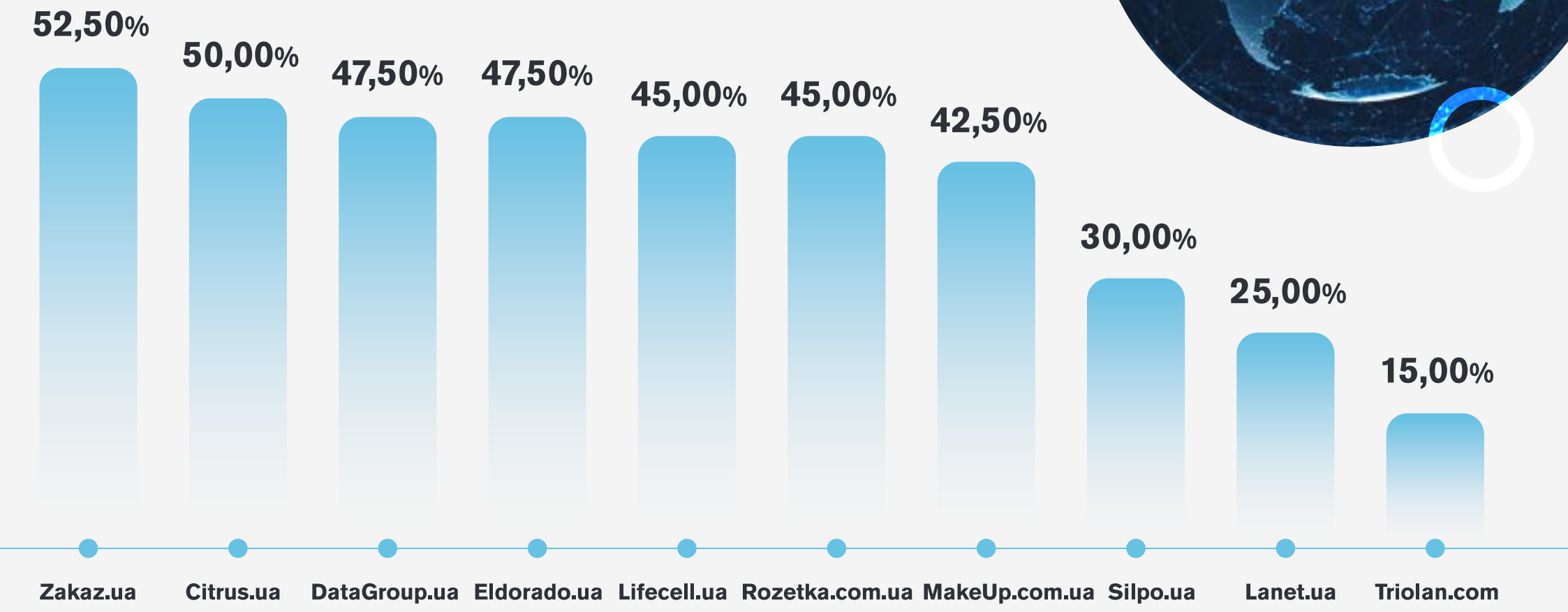
Мета дослідження *Індекс захисту персональних даних* — **проаналізувати політику компаній щодо дотримання цифрових прав користувачів з акцентом на захисті персональних даних.** З одного боку, результати дослідження допоможуть визначити, які українські приватні технологічні компанії можна зарахувати до умовної категорії **«чемпіони» з дотримання цифрових прав користувачів.** З іншого боку, результати продемонструють, яким компаніям **варто переглянути свою корпоративну політику й зробити більший акцент на захисті користувачів** та їхніх невідчужуваних прав в онлайн-просторі.

У розробці дослідження команда проєкту взяла за основу методологію визнаного у світі проєкту **Ranking Digital Rights**, яку розробила американська неурядова організація New America. Цю методологію адаптували до українських реалій політики захисту цифрових прав користувачів.

КОРОТКІ ВИСНОВКИ ДОСЛІДЖЕННЯ

Індекс захисту персональних даних — 2021

*Від 100%


52,50%
50,00%
47,50%
47,50%
45,00%
45,00%
42,50%
30,00%
25,00%
15,00%
Zakaz.ua
Citrus.ua
DataGroup.ua
Eldorado.ua
Lifecell.ua
Rozetka.com.ua
MakeUp.com.ua
Silpo.ua
Lanet.ua
Triolan.com

КОРОТКІ ВИСНОВКИ ДОСЛІДЖЕННЯ

- Найкращі результати серед 20 досліджуваних компаній **продемонстрували Olx.ua з показником 77,5%, Ukr.net та Foxtrot.ua з показником 70% балів кожна з максимально можливих 100%** як відображення стану корпоративної політики приватності та захисту персональних даних користувачів.

- Водночас навіть для Olx.ua, Ukr.net та Foxtrot.ua є простір для вдосконалення своєї корпоративної політики, зокрема в аспектах **дотримання принципу мінімізації даних,** які вони збирають про користувачів (Olx.ua), **публікації попередніх версій політики конфіденційності на сайтах** (Olx.ua, Ukr.net), надання можливості користувачам **отримати копію своїх персональних даних,** зазначення **часових меж відповідей на запити користувачів** (Ukr.net).

- Щонайменше **50% максимальної кількості балів отримали 12 із 20 приватних компаній за критерієм захисту персональних даних.** Корпоративну політику цих компаній оцінюють як середнього та вищого від середнього рівня в контексті забезпечення дієвого захисту персональних даних своїх клієнтів. До цих компаній **увійшли Kyivstar.ua, Comfy.ua, Allo.ua, Kasta.ua, Prom.ua, NovaPoshta.ua, Vodafone.ua, Zakaz.ua, Citrus.ua та вже згадані Olx.ua, Ukr.net та Foxtrot.ua.**

- Згаданим компаніям варто звернути увагу на **дотримання принципу мінімізації даних,** які вони збирають про користувачів, на **публікацію політики конфіденційності в простій та доступній** формі на своєму сайті, на чітке прописання **процесу передавання даних третім особам** тощо.

- **8 із 20 компаній, обраних для дослідження, набрали менше ніж 50%** балів з максимально можливих, що свідчить про нижчий за середній рівень захисту персональних даних, відображених у корпоративній політиці. Серед них — **Eldorado.ua, DataGroup.ua, Lifecell.ua, Rozetka.com.ua, Makeup.com.ua, Silpo.ua, Lanet.ua і Triolan.com.**

- Більшість із зазначених компаній мають значні **недоліки** в чотирьох категоріях дослідження — **від дотримання вимог національного законодавства до зручності користування сайтом та інклюзивністю.** Менеджменту цих компаній варто переглянути корпоративну політику приватності та захисту персональних даних, розробити й реалізувати план з посилення політики конфіденційності.

- На сайтах **4 компаній** (Vodafone.ua, Silpo.ua, Triolan.com, Lanet.ua) **немає відмітки для користувача про надання дозволу на оброблення його персональних даних,** хоча це одна з вимог законодавства.

- **10** досліджуваних компаній **не інформують своїх користувачів, впродовж якого часу ці компанії зберігатимуть інформацію про користувача.**

- На сайтах **4 компаній** (Triolan.com, Makeup.com.ua, Silpo.ua, Lanet.ua) **користувачі не мають можливості видалити свої збережені особисті дані.**

- **15** досліджуваних компаній **не описують умов видалення акаунту користувача** після припинення договору / за умов некористування акаунтом.

- **10** досліджуваних компаній **не вказують, де та як вони зберігають дані користувачів (розташування серверів).**

- Ознайомитися з результатами дослідження для **кожної з 20 приватних компаній** можна в анкеті за **посиланням *bit.ly/personaldataUA*.**

КОРОТКИЙ ВИКЛАД МЕТОДОЛОГІЇ ДОСЛІДЖЕННЯ

КОРОТКИЙ ВИКЛАД МЕТОДОЛОГІЇ ДОСЛІДЖЕННЯ

Мета дослідження *Індекс захисту персональних даних* — вивчити корпоративну політику підзвітності та прозорості провідних компаній приватного сектору в Україні на предмет дотримання ними цифрових прав людини в аспекті права на приватність та культури зберігання і розпорядження персональними даними користувачів.

В основі дослідження — прикладний аналіз і рейтингування на основі **роботи з відкритими джерелами даних та офіційними відповідями від приватних компаній** щодо їхньої політики приватності та захисту персональних даних. Етапи польового дослідження й аналізу охоплюють:

- збирання інформації щодо корпоративної політики компаній з відкритих джерел, а саме — **офіційних сайтів компаній приватного бізнесу;**
- створення та надсилання **інформаційного запиту** до компаній приватного бізнесу з **уточненням щодо їхньої політики у сфері приватності;**
- розроблення **анкети оцінювання отриманих даних**, що передбачає класифікацію запитань відповідно до чотирьох категорій дослідження;
- **аналізування отриманих даних і виставлення оцінок** відповідно до схваленої шкали оцінювання.

Команда проєкту сфокусувала свою увагу на вивченні чотирьох ключових аспектів корпоративної політики компаній приватного сектору:

1) дотримання вимог чинного законодавства України про персональні дані;

2) дотримання європейських стандартів щодо персональних даних;

3) технологічні аспекти роботи сайту;

4) зручність користування сайтом та інклюзивність.

Дослідження основане на загальнодоступних документах, що є у відкритому доступі на офіційних сайтах компаній. Доступ до цих документів може отримати будь-який користувач. Також дослідники вивчили технічні аспекти роботи офіційних сайтів компаній.

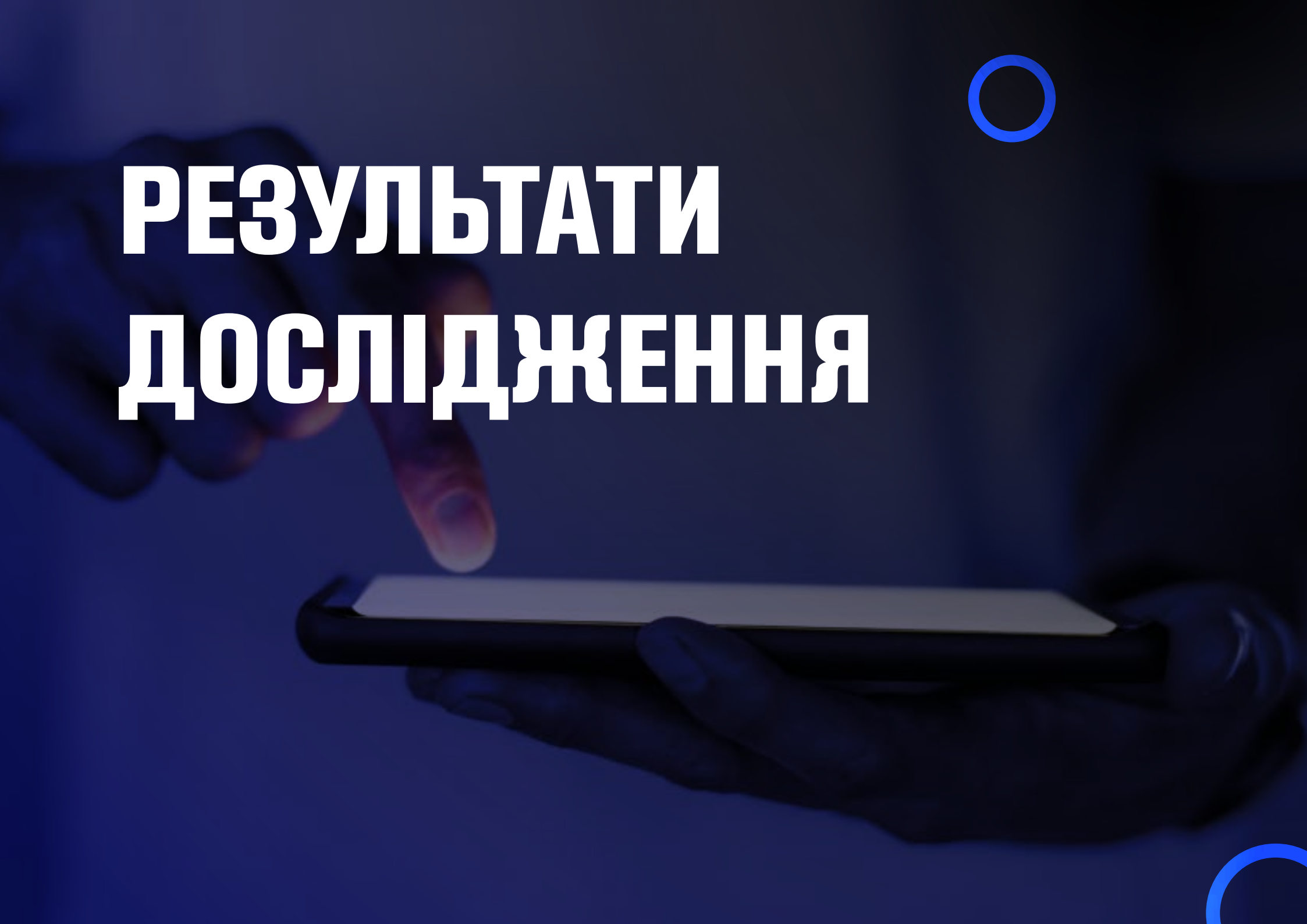
У першому виданні Індексу захисту персональних даних за 2021 рік дослідили 20 великих приватних компаній, що працюють в Україні. Ці компанії представляють телеком, провайдерів та онлайн-послуги.

Щоб оцінити корпоративну політику компаній за визначеними категоріями, команда проєкту розробила оцінювальну анкету. **Анкета містить 20 запитань.** Експерти проєкту ставили оцінку в кожному з індикаторів, обираючи між трьома можливими оцінками:

- **оцінка «0»** — інформації немає або ж вона недоступна / не виявлена, що вказує на ігнорування компанією цього питання / недотримання критерію захисту цифрових прав;
- **оцінка «0,5»** — інформація неповна, що вказує на часткове розкриття компанією політики в конкретному аспекті / часткове дотримання критерію захисту цифрових прав;
- **оцінка «1»** — інформація наявна, є вичерпною і зрозумілою для користувача / повне дотримання критерію захисту цифрових прав.

Оцінки за кожним індикатором виставляв один з експертів. Отримані результати за кожним індикатором затверджували другий і третій експерти. Результати корегували на основі отриманої інформації від компаній у відповідь на офіційний запит від ГО «Інтерньюз-Україна». **Фінальні оцінки (бали) порівнювали між собою й виводили у відсоткове співвідношення (%) максимальної кількості балів,** які могла набрати кожна з компаній.

Дослідження реалізувала ГО «Інтерньюз-Україна» за участю юристів та експертів з питань цифрових технологій. До робочої групи проєкту ввійшли Тетяна Авдеєва, Павло Бєлоусов, Лідія Волкова, Віталій Мороз, Аліна Правдиченко.



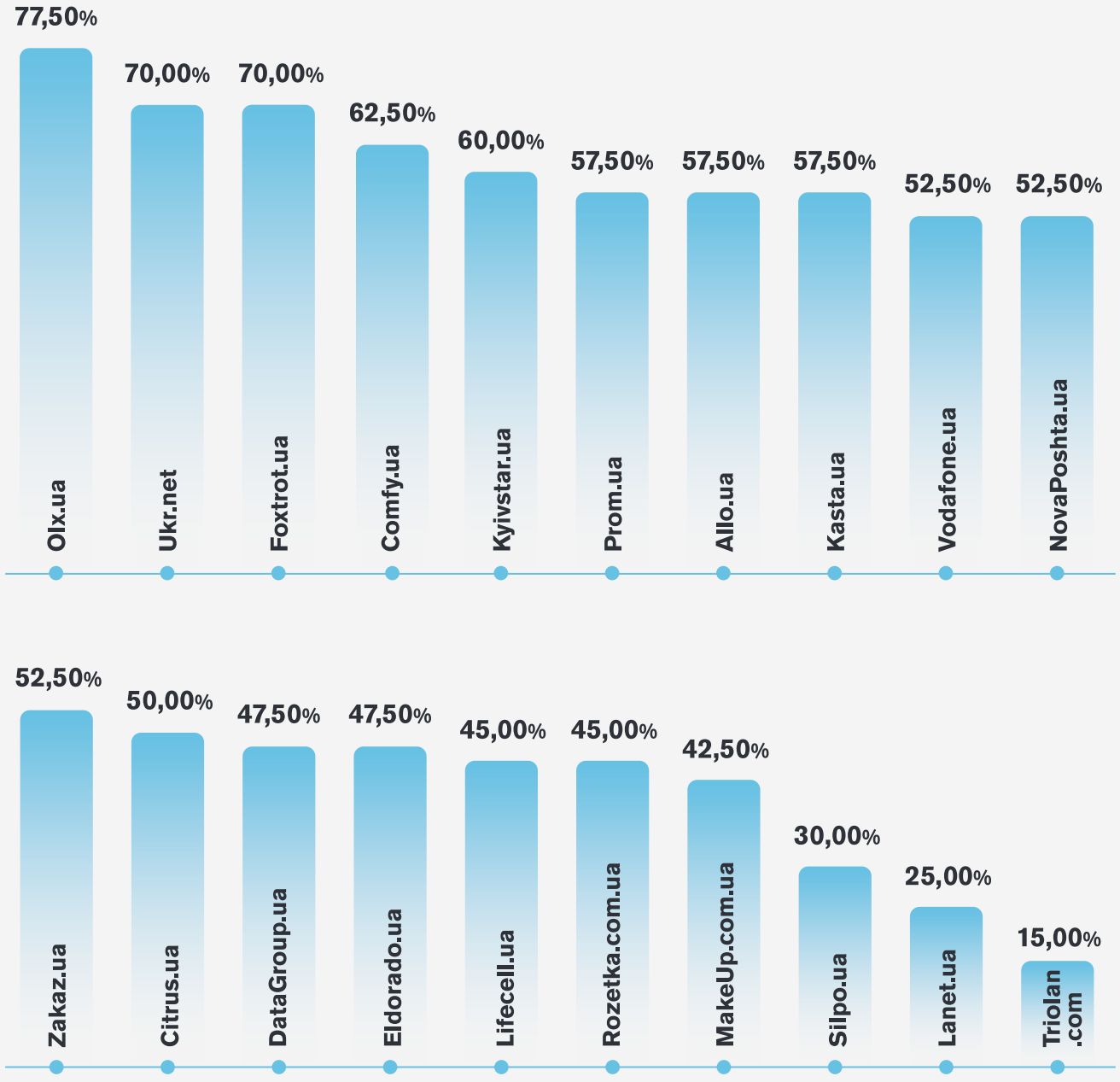
РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

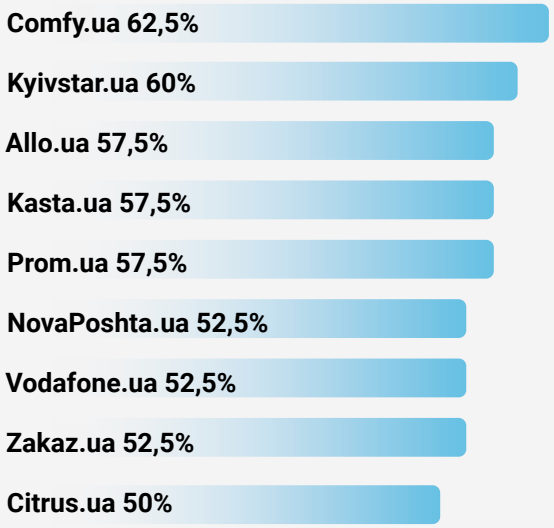
Зведені результати дослідження щодо дотримання цифрових прав користувачів в аспекті політики приватності та захисту персональних даних приватних компаній показують, що «чемпіонами» серед 20 компаній, обраних для дослідження, є компанії Olx.ua та Ukr.net. Вони отримали найвищі оцінки — відповідно 77,5% та 70% з максимально можливих 100% як відображення стану корпоративної політики приватності та захисту персональних даних.

Для цих двох компаній удосконалення корпоративної політики щодо приватності та захисту персональних даних можуть бути незначними, оскільки дизайн поточної політики добре продуманий та реалізований у більшості аспектів. Водночас для Olx.ua є простір для вдосконалення, зокрема це стосується дотримання принципу мінімізації даних, які вони збирають про користувачів, публікації попередніх версій політики конфіденційності на сайті. Для Ukr.net теж актуальне питання ознайомлення користувачів з попередніми версіями політики конфіденційності, зазначення дати публікації поточної версії. Компанія може чіткіше прописати положення щодо можливості користувачів отримати копію своїх персональних даних та вказати часові межі відповідей на запити користувачів.

Загалом 12 із 20 приватних компаній відповідають критеріям захисту персональних даних щонайменше на 50% максимальної кількості балів відповідно до методології дослідження. Відповідно корпоративна політика цих компаній оцінюється як середнього та вище від середнього рівня в контексті забезпечення дієвого захисту персональних даних своїх клієнтів.

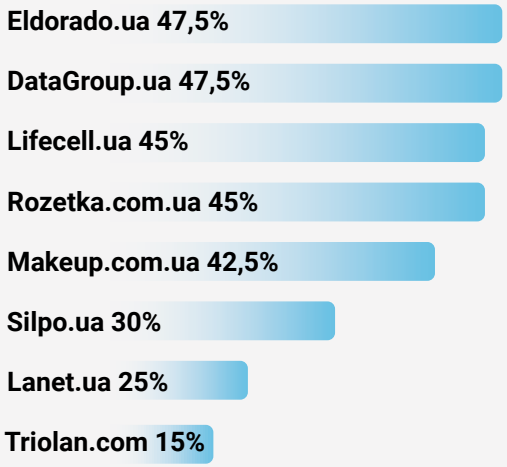


Для 10 компаній зведена оцінка є в межах від 50% до 70% усіх можливих балів за критеріями захисту персональних даних. Серед них:



Для багатьох із цих компаній варто звернути увагу на дотримання принципу мінімізації даних, які вони збирають про користувачів, публікацію політики конфіденційності в простій та доступній формі на своєму сайті. Для онлайн-сервісів, де продають товари та послуги, треба чітко прописати, як відбувається передавання даних третім особам. Нерідко бракує вичерпної інформації щодо безпечного збереження даних на серверах із зазначенням географічного розташування цих серверів. Компанії нечасто інформують користувачів, чи розроблена в них внутрішня політика / правила щодо роботи з персональними даними та їх захисту.

Вісім компаній не досягли позначки 50% усіх можливих балів за критеріями захисту персональних даних відповідно до методології дослідження. Серед них:



Дослідники зазначають, що в більшості з цих компаній є значні недоліки у всіх чотирьох категоріях — від дотримання вимог національного законодавства до зручності користування сайтом та інклюзивності. Зокрема, Lifecell.ua отримав украй низькі бали в категорії «Дотримання європейських стандартів». На сайті Lifecell.ua користувач не може чітко усвідомлювати, що він дає згоду на обробленя своїх даних. Замість чіткого опису політики конфіденційності компанія пропонує загальні умови користування телекомунікаційними послугами на 39 сторінок. Також компанія не вказує, чи можна надати запит у компанію й отримати копію своїх персональних даних.

У роботі популярного сервісу онлайн-покупок Rozetka.com.ua компанія не зазначає, як довго вона зберігатиме інформацію про користувача. Водночас Rozetka.com.ua намагається отримати від користувача максимально багато параметрів, включно з «у мене є дитина», хоча ці опції не є обов'язковими для надання послуг користувачу.

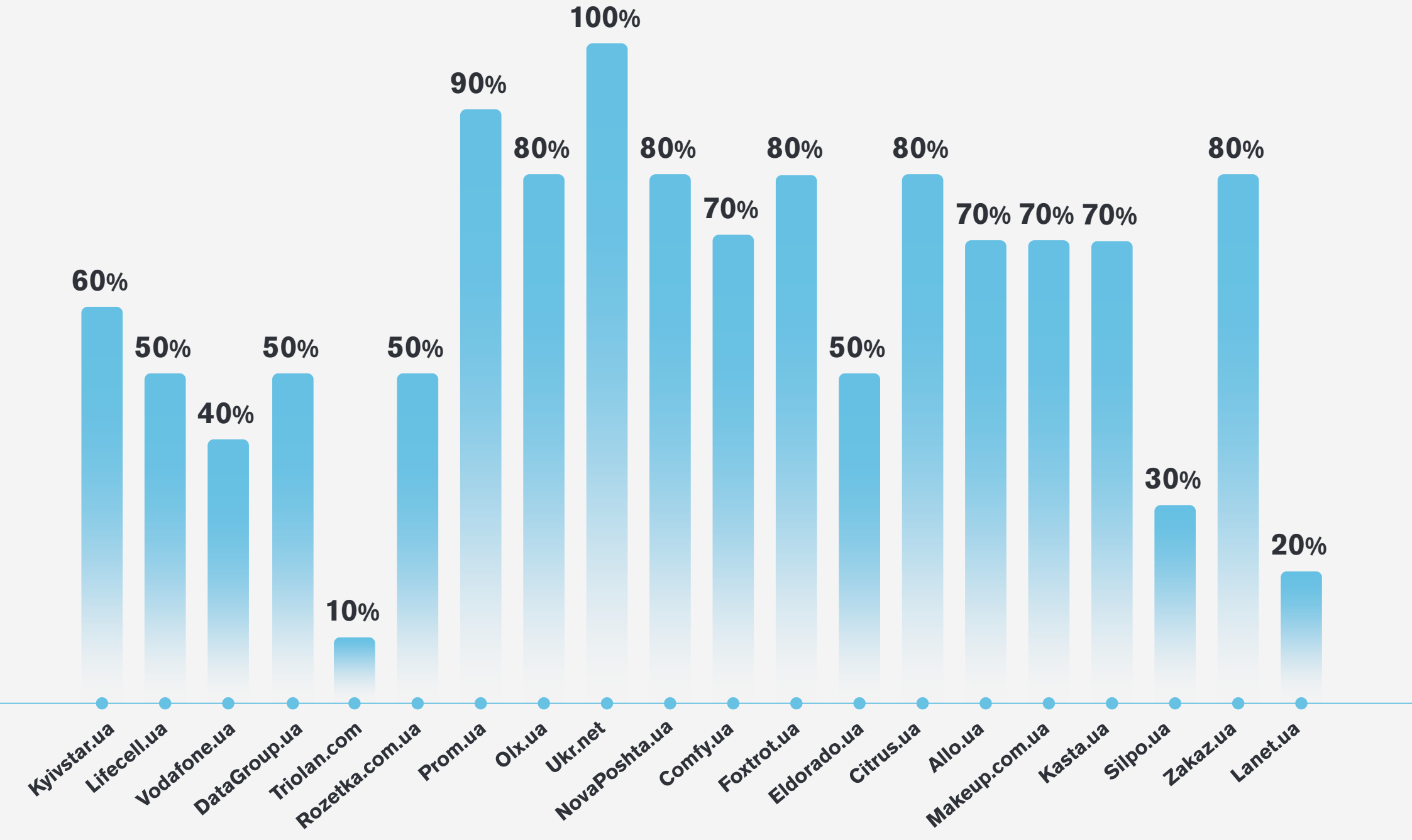
Менеджменту цих компаній варто переглянути корпоративну політику приватності та захисту персональних даних, розробити та реалізувати план з посилення політики конфіденційності.

Особливо варто зазначити про компанії, що отримали найменші бали. Ідеться про Triolan.com (15%), Lanet.ua (25%) та Silpo.ua (30%). Ці цифри свідчать про недостатнє усвідомлення компаніями важливості захисту персональних даних, а корпоративна політика конфіденційності та захисту персональних даних є щонайменше на початковому етапі їхнього впровадження.

Ознайомитися із заповненою дослідниками анкетою дослідження з оцінками щодо кожної з 20 компаній можна за посиланням *bit.ly/personaldataUA*.

Детальніші результати дослідження можна переглянути в розрізі кожної з чотирьох категорій відповідно до методології дослідження (детальніше про методологію на с. 21).

Категорія 1. Дотримання вимог чинного законодавства України про персональні дані



Результати в категорії № 1 «Дотримання вимог чинного законодавства»

У цій категорії більшість компаній отримали переважно вищі бали проти інших категорій. Для цього є цілком логічне пояснення: кожна з компаній працює у правовому полі українського законодавства й бере до уваги необхідність дотримувати положень регуляторних актів.

Ukr.net набрав у першій категорії 100% можливих балів, Prom.ua — 90%. Компанії, як-от Foxtrot.ua, NovaPoshta.ua, Olx.ua, Citrus.ua, Zakaz.ua, набрали 80% балів. Трохи менше — 70% — набрали ще чотири сервіси: Kasta.ua , Makeup.com.ua, Allo.ua та Comfy.ua.

Низькі бали, що свідчать про часткове недотримання компаніями вимог чинного законодавства у сфері захисту персональних даних, отримали Triolan.com (10%), Lanet.ua (20%) та Silpo.ua (30%). Цим компаніям варто критично переглянути політику конфіденційності та захисту персональних даних і погодити її з вимогами чинного законодавства.

У категорії № 1 дослідники оцінювали компанії відповідно до сформульованих запитань дослідження, зокрема:

- Чи є на сайті відмітка для користувача про надання дозволу на оброблення його персональних даних?
- Чи інформує компанія користувача про те, яку саме інформацію про нього збирає та яким чином її використовує?
- Чи вказує компанія термін, упродовж якого зберігатиме інформацію про користувача?
- Чи можуть користувачі самостійно видалити на сайті збережені особисті дані?
- Чи дотримує компанія принципу мінімізації даних, що відповідає меті оброблення цих даних?

Результати в категорії № 2 «Дотримання європейських стандартів»

Хоча європейські стандарти із захисту прав людини, а саме щодо захисту персональних даних, не є обов'язковими для компаній, які працюють в Україні, європейський регламент (GDPR) поширюється на територію інших країн, якщо взаємодія відбувається з громадянами ЄС. Багато українських компаній адаптують свою корпоративну політику з огляду на положення GDPR, на які також рівняється український законодавець у новому проєкті закону № 5628 про захист персональних даних. Очікується, що цей законопроєкт ухвалять депутати Верховної Ради України восени 2021 року.

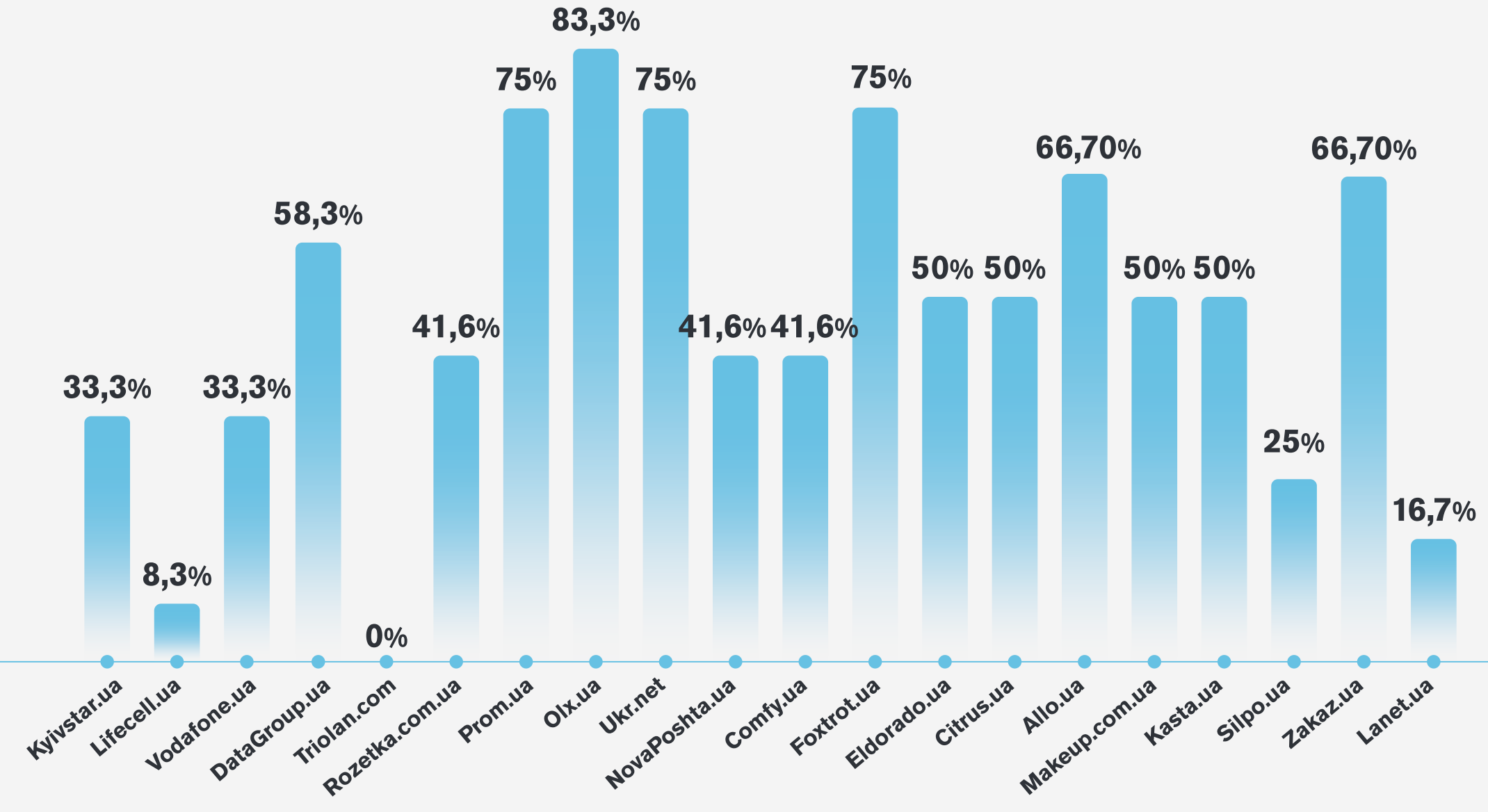
Загалом більшість досліджуваних компаній не набрали максимально високих балів у цій категорії, а частина сервісів отримали вкрай низькі оцінки. Найвищі бали набрали сервіси Ukr.net (83,5%), Foxtrot.ua, Olx.ua та Prom.ua (кожен по 75%).

Украй низькі бали отримали сервіси Lifecell.ua (8,3%), Lanet.ua (16,7%), Silpo.ua (25%). А провайдер Triolan не набрав у цій категорії жодного бала (0%).

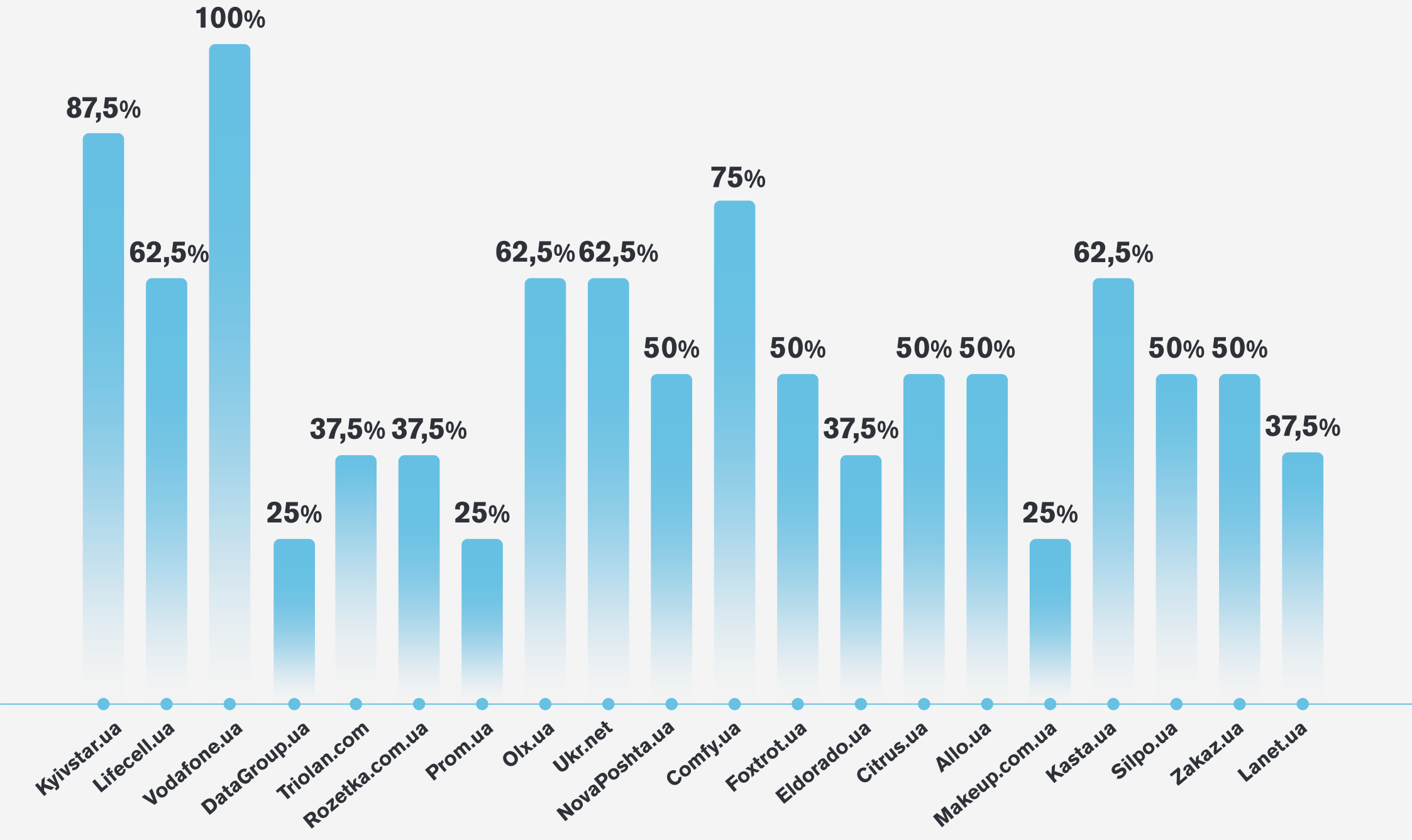
У категорії № 2 дослідники оцінювали компанії відповідно до сформульованих запитань дослідження, зокрема:

- Чи дозволяє функціонал сайту користувачу чітко усвідомлювати, що він дає згоду на оброблення своїх даних?
- Чи надана інформація про політику конфіденційності на сайті у стислій, прозорій, зрозумілій та легкодоступній формі?
- Чи можуть користувачі на сайті ознайомитися з попередніми версіями політики конфіденційності та зі змінами в оновленій версії політики конфіденційності?
- Чи описує компанія умови видалення акаунту користувача після припинення договору / за умов некористування акаунтом?
- Чи пояснює компанія, як відбувається передавання даних користувача третім особам?
- Чи може користувач надати запит у компанію й отримати копію своїх персональних даних?

Категорія 2. Дотримання європейських стандартів щодо персональних даних



Категорія 3. Технологічні аспекти роботи сайту



Результати в категорії № 3 «Технологічні аспекти роботи сайтів»

За результатами дослідження, корпоративна політика щодо безпечного користування сайтом є пріоритетом для таких компаній, як Vodafone.ua (100%), Kyivstar.ua (87,5%) та Comfy.ua (75%), — взаємодії користувачів та їхні персональні дані переважно захищені.

Найгірші бали отримали DataGroup.ua, Makeup.com.ua та Prom.ua — кожен по 25%, що вимагає від компаній залучити технічних фахівців, аби усунути проблеми з відсутністю посиленого захисту від несанкціонованого доступу (як-от двофакторна автентифікація під час входу), інформування про безпечне збереження даних користувачів (сервери).

У категорії № 3 дослідники оцінювали компанії відповідно до сформульованих запитань дослідження, зокрема:

- Чи використовує компанія протокол захищеного з'єднання https для сайту?
- Де та як компанія зберігає дані користувачів?
- Чи доступна користувачам опція посиленого захисту від несанкціонованого доступу?
- Чи можуть користувачі переглядати та керувати авторизаціями на сайті, коли і звідки заходили в кабінет користувача?

Результати в категорії № 4 «Зручність користування та інклюзивність»

Зручність користування та інклюзивність вказують на дизайн-мислення компаній, що пропонують користувачам свої сайти для взаємодії.

Найкращі показники за результатами дослідження продемонстрував сервіс Olx.ua з оцінкою 80%. Чотири компанії — Kyivstar.ua, Lifecell.ua, Comfy.ua, Foxtrot.ua — набрали по 70% кожна.

Найнижчу оцінку отримав сервіс доставки їжі — Zakaz.ua (10%). За ним ідуть три компанії з оцінкою 20% — Makeup.com.ua, Citrus.ua та Triolan.com.

У категорії № 4 дослідники оцінювали компанії відповідно до сформульованих запитань дослідження, зокрема:

- Чи можуть користувачі швидко і зручно знайти на сайті інформацію про захист персональних даних на сайті?
- Чи може користувач ознайомитися з внутрішньою політикою / правилами компанії щодо роботи з персональними даними та їх захисту?
- Чи інформує компанія про часові межі реакції на запити користувачів, що стосуються персональних даних?
- Чи може користувач отримати від компанії відповіді на свої запити через службу підтримки за допомогою принаймні двох засобів комунікації (гаряча лінія, імейл, чатбот)?
- Чи компанія надає змогу користуватися сайтом людям з інвалідністю?

У який спосіб отримано ці результати?

Результати цього дослідження отримано на основі збирання інформації з відкритих джерел даних (офіційні вебсайти компаній) та офіційних відповідей компаній на офіційні запити. На першому етапі команда проєкту визначила перелік досліджуваних компаній, провела моніторинг офіційних вебсайтів компаній.

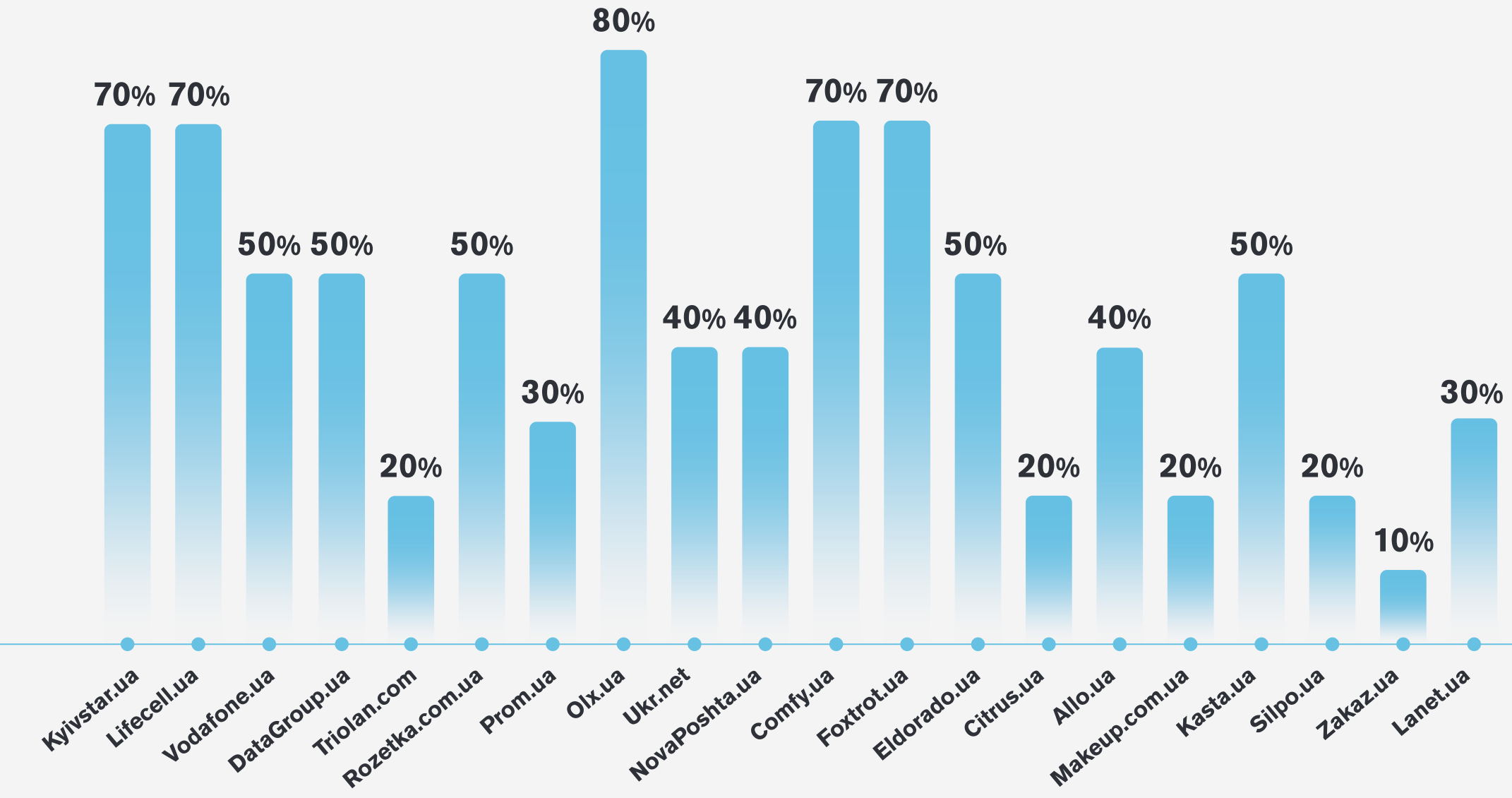
Експерти проєкту зібрали інформацію про корпоративну політику, дослідивши офіційні вебсайти компаній. Проаналізували отримані дані, проставили оцінки (бали) і згодом затвердили отримані результати (анкета).

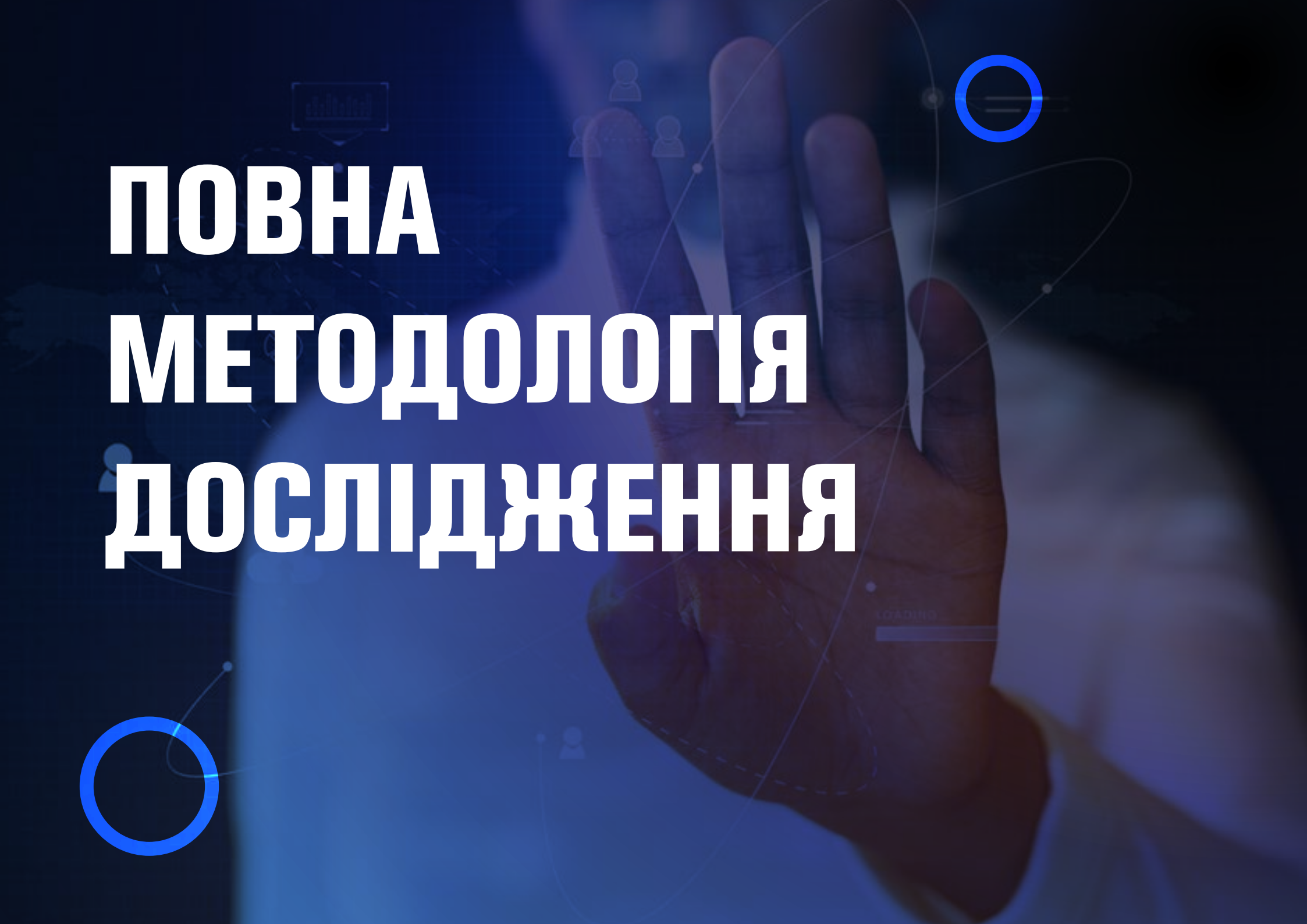
Для корегування отриманих результатів команда проєкту створила та надіслала офіційні інформаційні запити від ГО «Інтерньюз-Україна» на адресу компаній з уточнювальними запитаннями про їхню політику у сфері приватності та захисту персональних даних. Запит надсилали на офіційну поштову адресу компанії, а також дублювали на офіційний імейл компанії, отриманий з відкритих джерел.

Упродовж 40 днів з моменту надсилання таких запитів команда дослідження отримали близько 30% відповідей — тільки 8 із 20 компаній надали відповіді станом на кінець червня 2021 року. Відповіли такі компанії: Olx.ua (ТОВ «ЄМАРКЕТ УКРАЇНА»), Prom.ua (ТОВ «УАПРОМ»), Vodafone.ua (ПрАТ «ВФ УКРАЇНА»), Kyivstar.ua (ПАТ «Київстар»), NovaPoshta.ua (ТОВ «Нова Пошта»), Silpo.ua (ТОВ «СІЛЬПО-ФУД»), Comfy.ua (ТОВ «КОМФІ-ТРЕЙД»), Lifecell.ua (ТОВ «Лайфселл»). Решта 12 компаній, імовірно, не надали відповідь на запит, адже команда проєкту не отримала від цих компаній відповіді в період 40 днів з моменту надсилання запиту.

Результати дослідження відображають політику компаній у сфері приватності та захисту персональних даних станом на липень 2021 року — період аналізу даних.

Категорія 4. Зручність користування та інклюзія




ПОВНА
МЕТОДОЛОГІЯ
ДОСЛІДЖЕННЯ

ПОВНА МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

Індекс захисту персональних даних — інструмент вивчення корпоративної політики провідних компаній приватного сектору в Україні щодо дотримання ними цифрових прав користувачів в аспекті захисту персональних даних. Дослідження провела ГО «Інтерньюз-Україна» за участю експертів з питань цифрових технологій та юристів. До робочої групи проєкту ввійшли Тетяна Авдеєва, Павло Бєлоусов, Лідія Волкова, Віталій Мороз та Аліна Правдиченко.

Предмет дослідження

Корпоративна політика підзвітності та прозорості провідних компаній приватного сектору в Україні в розрізі дотримання ними цифрових прав користувачів.

Мета дослідження

Вивчити корпоративну політику підзвітності та прозорості провідних компаній приватного сектору в Україні на предмет дотримання ними цифрових прав людини в аспекті права на приватність і культури зберігання персональних даних користувачів та розпорядження ними.

Ключові методи дослідження

В основі дослідження — прикладний аналіз і рейтингування на основі роботи з відкритими джерелами даних та офіційними відповідями від компаній. Етапи польового дослідження й аналізу охоплюють:

- збирання інформації щодо корпоративної політики компаній з відкритих джерел, а саме — офіційних сайтів компаній приватного бізнесу;
- створення та надсилання інформаційного запиту до компаній приватного бізнесу з уточненням щодо їхньої політики у сфері приватності;
- розроблення анкети оцінювання отриманих даних, що передбачає класифікацію запитань відповідно до чотирьох категорій дослідження;
- аналізування отриманих даних і виставлення оцінок відповідно до схваленої шкали оцінювання.

Критерії оцінювання відповідно до методології дослідження

Команда проєкту сфокусувала свою увагу на вивченні чотирьох ключових аспектів корпоративної політики компаній приватного сектору:

1. **Дотримання вимог чинного законодавства України про персональні дані.** Визначається за критеріями, серед яких:
   - компанія передбачила проставлення відмітки про надання дозволу на оброблення своїх персональних даних для користувача;
   - компанія забезпечила користувачу право знати, яку саме інформацію про нього збирають і яким чином її використовують;
   - компанія зазначає термін, упродовж якого зберігатиме інформацію про користувача
   - компанія передбачила, що користувач може видалити на сайті свої збережені дані;
   - компанія дотримує принципу мінімізації даних.
2. **Дотримання європейських стандартів щодо персональних даних.** Визначається за критеріями, серед яких:
   - користувач чітко усвідомлює, що дає згоду на оброблення своїх даних;
   - інформація про політику конфіденційності має бути надана користувачу в стислій, прозорій, зрозумілій та легкодоступній формі, з використанням чітких і простих формулювань;
   - компанія передбачила опцію ознайомлення користувачів з попередніми версіями політики конфіденційності та зі змінами в оновленій версії політики конфіденційності;
   - компанія описує умови видалення акаунту користувача після припинення договору / за умов некористування акаунтом;
   - компанія пояснює, як відбувається передавання даних користувача третім особам;
   - компанія надає змогу користувачам надсилати запит на отримання копії своїх персональних даних.
3. **Технологічні аспекти роботи сайту.** Визначається за критеріями, серед яких:
   - компанія передбачила в роботі сайту використання протоколу захищеного з'єднання https;

- компанія передбачила хостинг серверів на території країн, де не діє репресивне законодавство щодо інтернету й доступ до даних захищений законом;
- компанія передбачила для користувачів можливість посиленого захисту від несанкціонованого доступу до кабінету користувача;
- компанія передбачила можливість користувачам переглядати історію відвідувань, коли і звідки заходили в кабінет користувача.

4. Зручність користування сайтом та інклюзивність. Визначається за критеріями, серед яких:

- користувач може швидко і зручно знайти на сайті інформацію про захист персональних даних;
- користувач може ознайомитися з внутрішньою політикою / правила компанії щодо роботи з персональними даними та їх захисту;
- користувач може отримати від компанії відповіді на свої запити через службу підтримки;
- компанія інформує про часові межі реакції на запити користувачів, що стосуються персональних даних;
- компанія надає змогу користуватися сайтом людям з інвалідністю.

Щоб оцінити корпоративну політику компаній за визначеними категоріями, команда проєкту розробила оцінювальну анкету. Анкета містить 20 запитань. Експерти проєкту ставлять оцінку в кожному з пунктів, обираючи між трьома можливими оцінками:

- **оцінка «0»** — інформації немає або ж вона недоступна / не виявлена, що вказує на ігнорування компанією цього питання / недотримання критерію захисту цифрових прав;
- **оцінка «0,5»** — інформація неповна, що вказує на часткове розкриття компанією політики в конкретному аспекті / часткове дотримання критерію захисту цифрових прав;
- **оцінка «1»** — інформація наявна, є вичерпною і зрозумілою для користувача / повне дотримання критерію захисту цифрових прав.

Критерії обрання компаній для дослідження

Усього під час першого етапу проєкту 2021 року об'єктами дослідження стали 20 компаній, поділені на дві групи: до першої групи належить 6 компаній, що представляють операторів мобільного зв'язку та провайдерів. До другої групи — 14 компаній, що надають послуги користувачам за допомогою електронних сервісів за умов реєстрації на сайті або ж без неї. Поділ компаній зумовлений особливістю надання послуг користувачам та обсягу персональної інформації, які компанії зберігають та якими розпоряджаються.

Ключові критерії вибору компаній першої групи (телеком):

- компанії надають користувачам послуги з мобільного зв'язку / доступу до інтернету;
- компанії є лідерами ринку й мають офіційні сайти з інформацією щодо політики користування;
- для ідентифікації користувачів компанії збирають їхні персональні дані.

Ключові критерії вибору компаній другої групи (сервісні компанії):

- в основі комерційної діяльності компаній є робота сайту, через який користувачам надають послуги / продають товари;
- сайти компаній входять до найпопулярніших сайтів серед українських користувачів за результатами досліджень, зокрема й відповідно до результатів дослідження Kantar CMeter станом на лютий 2021 року;
- користувачам треба реєструватися на сайтах компаній із переданням персональної інформації, аби скористатися послугами компаній, або послуги надають без реєстрації, однак це все одно передбачає передавання персональних даних.

Звідки беруться дані дослідження?

Дослідження є можливим завдяки аналізуванню зібраного масиву даних. Дані отримано з відкритих джерел (офіційних вебсайтів компаній) та через відповіді компаній на офіційні запити від дослідників. Неможливість отримати офіційні дані чи відсутність даних враховано під час формування висновків дослідження.

Два ключові способи отримання даних:

1) збирання та аналізування інформації з відкритих джерел за допомогою моніторингу офіційних вебсайтів компаній приватного сектору;
2) формування та надсилання інформаційного запиту до компаній приватного бізнесу з уточненням щодо їхньої політики у сфері приватності. Запити складали відповідно до вимог українського законодавства й надсилали поштою. Пара-

лельно, запити були продубльовані на офіційні імейли компаній. Команда проєкту очікувала отримати відповіді від компаній в період 40 днів з моменту надсилання запиту.

Як працювала команда дослідження?

До складу команди дослідження ввійшло шестеро фахівців у сфері цифрових технологій та юристи. Команда проєкту відповідає за адаптацію методології дослідження, проведення польового етапу, аналізування результатів на основі отриманих даних та представлення результатів проєкту.

Команда проєкту сформована в межах проєкту «Прозоре звітування у сфері телекомунікацій: на захисті приватності українських користувачів», що реалізується ГО «Інтерньюз-Україна» за підтримки Міжнародного фонду «Відродження» та Європейського Союзу в межах спільної ініціативи EU4USociety.

Як затверджують результати дослідження?

Команда проєкту використовувала підхід подвійної експертної оцінки (peer review) отриманих результатів. Один з експертів виставляє оцінки (бали), а згодом другий і третій експерти затверджують результати. Результати корегували на основі отриманої інформації від компаній у відповідь на офіційний запит від ГО «Інтерньюз-Україна». Фінальні оцінки (бали) порівнювали між собою і виводили у відсоткове співвідношення (%) максимальної кількості балів, які могла набрати кожна з компаній.

Як виглядає фінальний продукт дослідження?

Повний текст дослідження, так само як і короткі висновки, опубліковані у вигляді звіту на окремому сайті проєкту, є доступними публічно в онлайні, а також надіслані кожній із приватних компаній, що була об'єктом дослідження.

Запитання анкети в оцінюванні компаній

Команда проєкту розробила анкету, що складається з 20 запитань, розподілених серед чотирьох ключових категорій. За результатами відповіді на кожне запитання, експерт ставить одну з трьох можливих оцінок:

- **оцінка «0»** — інформації немає або ж вона недоступна / не виявлена, що вказує на ігнорування компанією цього запитання / недотримання критерію захисту цифрових прав;
- **оцінка «0,5»** — інформація неповна, що вказує на часткове розкриття компанією політики в конкретному аспекті / часткове дотримання критерію захисту цифрових прав;
- **оцінка «1»** — інформація наявна, є вичерпною і зрозумілою для користувача / повне дотримання критерію захисту цифрових прав.

Дотримання вимог законодавства України про персональні дані (5 запитань):

1. Чи є на сайті відмітка для користувача про надання дозволу на оброблення його персональних даних?
2. Чи інформує компанія користувача про те, яку саме інформацію про нього збирає та яким чином її використовує?
3. Чи вказує компанія термін, упродовж якого зберігатиме інформацію про користувача?
4. Чи можуть користувачі самостійно видалити на сайті збережені особисті дані?
5. Чи дотримується компанія принципу мінімізації даних, що відповідає меті оброблення цих даних?

Дотримання європейських стандартів щодо персональних даних (6 запитань):

1. Чи дозволяє функціонал сайту користувачу чітко усвідомлювати, що він дає згоду на оброблення своїх даних?
2. Чи надана інформація про політику конфіденційності на сайті у стислій, прозорій, зрозумілій та легкодоступній формі?
3. Чи можуть користувачі на сайті ознайомитися з попередніми версіями політики конфіденційності та зі змінами в оновленій версії політики конфіденційності?
4. Чи описує компанія умови видалення акаунту користувача після припинення договору / за умов некористування акаунтом?
5. Чи пояснює компанія, як відбувається передавання даних користувача третім особам?
6. Чи може користувач надати запит у компанію й отримати копію своїх персональних даних?

Технологічні аспекти роботи сайту (4 запитання):

1. Чи використовує компанія протокол захищеного з'єднання https для сайту?
2. Де та як компанія зберігає дані користувачів?
3. Чи доступна користувачам опція посиленого захисту від несанкціонованого доступу?
4. Чи можуть користувачі переглядати та керувати авторизаціями на сайті, коли і звідки заходили в кабінет користувача?

Зручність користування та інклюзивність (5 запитань):

1. Чи можуть користувачі швидко і зручно знайти на сайті інформацію про захист персональних даних?
2. Чи може користувач ознайомитися з внутрішньою політикою / правилами компанії щодо роботи з персональними даними та їх захисту?
3. Чи інформує компанія про часові межі реакції на запити користувачів, що стосуються персональних даних?
4. Чи може користувач отримати від компанії відповіді на свої запити через службу підтримки за допомогою принаймні двох засобів комунікації (гаряча лінія, імейл, чатбот)?
5. Чи компанія надає змогу користуватися сайтом людям з інвалідністю?

Пояснення критеріїв оцінки

Що ми розуміємо під «дотриманням вимог чинного законодавства України про персональні дані»?

1. **Наявність згоди користувача** є ключовою передумовою оброблення його персональних даних. Закон «Про захист персональних даних» (стаття 2) визначає згоду як добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на оброблення її персональних даних відповідно до сформульованої мети їх оброблення, висловлене в письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. У сфері електронної комерції згоду суб'єкта персональних даних можна надати під час реєстрації в інформаційно-телекомунікаційній системі суб'єкта електронної комерції, проставивши відмітку **про надання дозволу** на оброблення своїх персональних даних відповідно до сформульованої мети їх оброблення, **за умови, що така система не обробляє персональні дані до моменту проставлення відмітки.** Тобто ключовими моментами під час оцінювання цього компоненту ми вважаємо наявність активних дій користувача з надання згоди та неможливість скористатися послугою за відсутності таких дій. Фактично, йдеться про неможливість отримати послуги без натискання певних кнопок / проставлення відповідних відміток. За таких умов оцінюваний суб'єкт отримає 1 бал, за умови часткового дотримання зазначених критеріїв — 0,5 бала.
2. Ключовим правом суб'єкта персональних даних є **право знати, яку інформацію про нього збирають та яким чином її використовують.** Водночас закон прямо встановлює, що інформацію про власника персональних даних (тобто не просто про сайт, який збирає персональні дані, а про конкретну фізичну або юридичну особу), про склад та зміст зібраних персональних даних, права користувача ресурсу, мету збору персональних даних та осіб, яким передаються персональні дані, треба надати в момент збору персональних даних (стаття 12 ЗУ «Про захист персональних даних»). Зазвичай усі зазначені запитання розкриваються в політиці конфіденційності, яку надають для ознайомлення користувачу разом з можливістю надати згоду на оброблення персональних даних. З огляду на це суб'єкт оцінювання отримає 1 бал за наявності на його сайті політики конфіденційності, що містить усі наведені запитання, та за умови, що користувач ознайомиться з цією політикою до того, як передасть свої персональні дані. 0,5 бала отримають суб'єкти, які відповідають переліченим критеріям частково.
3. **Компанія зазначає строки зберігання даних.** Українське законодавство встановлює окремі вимоги щодо строку оброблення / збереження персональних даних. Персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, **не довше, ніж це необхідно для законних цілей, з якими їх збирали чи надалі обробляли** (стаття 6 ЗУ «Про захист персональних даних»). Закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на оброблення цих даних або законом, **є підставою для видалення даних** (стаття 12). Отже, зазначати строки зберігання даних украй важливо, і це має бути відображено на сайті компанії. Відповідно 1 бал отримають компанії, які прямо зазначають термін зберігання інформації про користувача, 0,5 — якщо термін нечітко вказано або приховано на сайті, 0 — якщо згадки немає.
4. Закон «Про захист персональних даних» прямо встановлює, що **згоду на оброблення персональних даних можна відкликати в будь-який час** (стаття 8). На практиці це означає, що технічно система надає змогу видаляти персональні дані (має бути відповідна кнопка / опція в інтерфейсі) / описаний прозорий механізм видалення персональних даних або принаймні контактна адреса, за якою можна звернутись із запитом про видалення персональної інформації. З огляду на це 1 бал отримують суб'єкти, сервіси яких містять прямі та недвозначні можливості для видален-

ня персональних даних (відповідні кнопки або інструкції), 0,5 бала отримають суб'єкти, сервіси яких дають змогу видаляти персональну інформацію за запитом.

5. Компанія дотримує **принципу мінімізації даних**, коли склад та зміст персональних даних, що збираються, мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їхнього оброблення. Одним із законодавчо встановлених принципів оброблення персональних даних є принцип мінімізації. Наприклад, **склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їхнього оброблення** (стаття 6 ЗУ «Про захист персональних даних»). Водночас мета оброблення даних має бути вказана в користувацькій угоді (політиці конфіденційності) та пов'язана з безпосередньо наданням запропонованих послуг. Це означає, що будь-яка компанія має збирати від користувачів лише ті дані, які є необхідними для надання послуг, та не питати зайвої інформації. З огляду на це суб'єкт оцінювання отримає 1 бал у разі повного дотримання принципу мінімізації та 0,5 бала в разі часткового дотримання.

Що ми розуміємо під «дотриманням європейських стандартів щодо персональних даних»?

Українське законодавство у сфері захисту персональних даних перебуває на шляху трансформації. Однією з причин цього є прагнення відповідати європейським стандартам, зокрема правилам GDPR — General Data Protection Regulation (Загальному регламенту про захист даних), що набрав чинності в Європейському Союзі 2018 року. Цей регламент значною мірою посилює права користувачів насамперед завдяки принципам простоти та зрозумілості. На сьогодні застосування GDPR не є обов'язковим на території України, але, враховуючи, що багато українських компаній можуть надавати свої послуги європейським користувачам, а також помітні кроки України в євроінтеграції, цілком доцільно оцінити, наскільки українські компанії є дружніми до користувачів та дотримують європейських стандартів.

1. Одним з таких стандартів є **стандарт очевидності згоди**. Відповідно до статті 7 GDPR, якщо суб'єкт даних надає згоду в контексті письмової декларації, що також стосується інших запитань, запит на надання згоди треба подавати у формі, що чітко відрізняється від інших запитань, у зрозумілій та доступній формі. Це означає, що **користувач має чітко усвідомлювати, що він дає згоду на оброблення своїх даних**, і опція надання такої згоди має бути відокремлена від усіх інших можливих дій (наприклад, за допомогою окремої кнопки, проставляння спеціальної відмітки тощо). Водночас не відповідатимуть стандарту застереження на кшталт «Натискаючи кнопку "Підтвердити замовлення", я даю згоду на оброблення своїх персональних даних» або «Продовжуючи користуватись сайтом, ви даєте згоду на оброблення своїх персональних даних», оскільки вони не є чітко відокремленими від інших питань або дій. Так само автоматично проставлена відмітка про надання згоди не вважається такою, що відповідає стандарту, оскільки користувач може її зняти, а може і не помітити.

2. **Політика конфіденційності** багатьох українських сайтів **зазвичай написана доволі сухою, важкозрозумілою юридичною мовою.** Натомість GDPR встановлює стандарти для інформування користувачів про використання їхніх персональних даних. Відповідно до статті 12, інформацію про політику конфіденційності треба надавати користувачу **в стислій, прозорій, зрозумілій та легкодоступній формі,** зокрема інформацію, спеціально призначену для дитини. Фактично, ідеться про те, що звичайний користувач, який не є юристом чи спеціалістом у сфері персональних даних, має легко зрозуміти, хто і як використовуватиме інформацію про нього.

3. Компанія передбачала опцію ознайомлення користувачів з можливістю переглядати **оновлення (версії) політики конфіденційності.** Це дає користувачеві змогу порівнювати зміни, які компанія впровадила щодо політики персональних даних, та за потреби скористатися своїм правом на відкликання згоди на оброблення.

4. Якщо немає більше потреби в персональних даних для цілей, для яких їх збирали чи іншим чином опрацьовували, **персональні дані мають бути стертими без будь-якого необґрунтованого затримання** (стаття 17 GDPR). Припинення договору або некористування акаунтом протягом тривалого часу в певних випадках може свідчити про те, що ціль збирання персональних даних більше не є актуальною, відповідно підстави для оброблення таких даних також відсутні. Саме тому важливо, **чи описує компанія умови видалення акаунту користувача після припинення договору / за умов некористування акаунтом.**

5. Компанія має право **передавати дані користувача третім особам за умови його згоди.** Під час отримання персональних даних користува-

ча мають поінформувати про одержувачів чи категорії одержувачів персональних даних (стаття 13 GDPR). Крім того, у GDPR детально регламентовані умови передавання даних до третьої країни чи міжнародної організації. Отже, **пояснення процесу передавання даних користувача третім особам** вбачається цілком важливим.

6. **Суб'єкт персональних даних має право отримати копії опрацьовуваних персональних даних** (стаття 15 GDPR). Відповідно суб'єкт може не лише знати про перелік таких даних, а й чітко бачити весь масив інформації, що опрацьовується. Великі міжнародні платформи надали своїм користувачам таку опцію кілька років тому.

Що ми розуміємо під «технологічними аспектами роботи сайту»?

Взаємодія користувачів із сайтами компаній передбачає **захищеність користувача від можливих шкідливих впливів та витоків інформації.** Сучасні стандарти захисту сайтів, їхніх серверів стають необхідністю, вони мають бути відображені як в архітектурі технічного складника роботи компаній, так і в роботі самих сайтів. Крім того, сайти повинні передбачати технічні можливості захисту на рівні користувача.

Отже, до базових критеріїв технічного складника належить можливість відвідувати сайти, що **працює на основі протоколу захищеного з'єднання https** за допомогою TLS-сертифіката. **Сервери компанії розташовані на території країн,** де не діє репресивне законодавство щодо інтернету й доступ до даних захищений законом, що мінімізує ризики несанкціонованого доступу до інформації на цих серверах і відповідно до персональних даних користувачів.

На рівні контролю користувачами за своїми даними відповідальні компанії **надають користувачам змогу переглядати історію відвідувань,** бачити, коли і звідки вони заходили на свій акаунт. Щоб захистити користувача від несанкціонованого доступу до акаунту, компанія здатна **забезпечити посилений захист** (наприклад, опція двофакторної аутентифікації (2ФА), авторизація через sms чи авторизація за IP-адресою) під час входу в особистий акаунт. Що ми розуміємо під «зручністю користування та інклюзивністю»?

Зручність користування сайтом, або ж юзабиліті, відповідає на потребу користувача **швидко й без ускладнень знаходити інформацію, яку він потребує,** посилання на цю інформацію відображені на першій сторінці сайту й видимі на тлі іншого змісту сайту. Компанії здатні акцентувати на захисті персональних даних у такий спосіб:

- публікувати на сайті **довідкову інформацію** про захист персональних даних;
- розробити та впровадити **внутрішню політику / правила компанії щодо роботи з персональними даними** та їх захисту;
- інформувати про **тривалість розгляду запитів**, що стосуються персональних даних;
- надавати користувачам змогу **контактувати з компанією через службу підтримки** в кілька зручних для користувача способів, як-от гарячу лінію, імейл, чатбот. Користування сервісами, а відповідно й сайтом передбачає врахування інтересів людей з інвалідністю. Щоб дотримувати принципу інклюзивності в організації роботи компанії, треба **надавати людям з інвалідністю (як-от людей з вадами зору чи слуху) послуги в зручній і доступній для них формі.** Зокрема, компанії мають передбачати можливість зв'язатися з оператором або чатботом у голосовому форматі, мати окрему версію вебсайту чи застосунку для людей з інвалідністю в разі, якщо сервіси компанії не можуть надаватися без такої версії.

Також компаніям треба розміщувати дисклеймер щодо існування такої версії, щоб користувачі знали про можливість використання додаткового (спеціального) функціоналу. Під час формування політики компанії треба уникати будь-яких дискримінаційних положень стосовно осіб з інвалідністю та всіляко сприяти інклюзивності.

ЩО ЗМІНИТЬСЯ ДЛЯ ПРИВАТНОГО СЕКТОРУ З УХВАЛЕННЯМ ЗАКОНОПРОЄКТУ № 5628

ЩО ЗМНІНИТЬСЯ ДЛЯ ПРИВАТНОГО СЕКТОРУ З УХВАЛЕННЯМ ЗАКОНОПРОЄКТУ № 5628

7 червня 2021 року в парламенті зареєстрували законопроєкт № 5628 про захист персональних даних. Серед представників громадських організацій, міжнародних партнерів, представників приватного сектору зазвучали голоси про необхідність його ухвалити. Що варто очікувати приватному сектору в разі ухвалення цього законопроєкту?

По-перше, усі **стандарти щодо захисту персональних даних тепер буде узгоджено** з вимогами Загального регламенту про захист даних ЄС (більш відомого як GDPR). На практиці це означає, що компанії, зареєстровані в межах ЄС, та українські сервіси муситимуть дотримуватися однакових вимог. Водночас споживачі, які мають надавати персональні дані, щоб отримати послугу, матимуть більше гарантій та захисту від зловживань. Зокрема, законопроєкт деталізує процедуру отримання згоди, а також встановлює механізм захисту від автоматизованого ухвалення рішень. Це покладатиме на компанії додатковий обов'язок щодо функціонування вебсайтів. Наприклад, так звані кукі-банери треба буде організувати належним чином, а поля для згоди не можна буде позначати пташечкою наперед — особа це муситиме зробити власноруч (що відповідає практиці Суду справедливості ЄС у Verbraucherzentrale Bundesverband Ev v Planet49 GmbH).

По-друге, компанії отримають широкий спектр **зобов'язань щодо здійснення перевірки відповідності процесів оброблення персональних даних міжнародним стандартам** у галузі прав людини (відповідно до практики ЄСПЛ щодо захисту приватності у M.L. and W.W. v Germany). Це здійснюватиметься у випадках систематичного й широкомасштабного аналізу персональних аспектів життя фізичних осіб (за допомогою автоматичного оброблення включно з профілюванням), оброблення чутливих даних чи моніторингу загальнодоступних місць або джерел. Окрім того, контролер муситиме призначити особу, відповідальну за захист персональних даних, яка матиме гарантії щодо неможливості її звільнити за надання оцінки щодо рівня захисту даних. Таким чином, компаніям щонайменше доведеться створювати окрему посаду для особи, яка опікуватиметься питанням захисту персональних даних.

По-третє, серед новацій законопроєкт також передбачає **розробку кодексів поведінки з питань захисту персональних даних**, що становитимуть комплекс правил, стандартів і процедур для галузей, секторів чи певних організацій. Такі кодекси можуть бути як спільними для кількох суб'єктів діяльності, так і окремими в кожній організації. По суті, це є виявом само- та співрегулівного механізму й сприятиме якіснішому запровадженню стандартів: представники бізнесу найкраще розуміють, як саме функціонує їхній продукт чи послуга, а тому зможуть найліпше організувати процедуру захисту даних, водночас не погіршуючи якості послуг.

Також законопроєкт пропонує норми для **захисту персональних даних у трудовій сфері, які обмежать роботодавців у можливості надмірно втручатись у приватність працівника.** Із важливих аспектів варто згадати заборону використовувати чутливі персональні дані для цілей, відмінних від оцінювання професійних компетентностей особи. Також окреме положення регулює можливість використовувати дані для проведення внутрішнього розслідування. Зокрема, зазначено, що в разі негативного результату такого розслідування працедавець повинен видалити дані, що цілком відповідає практиці ЄСПЛ у López Ribalda and Others v Spain. Зберігатися ж дані повинні до спливу строку позовної давності.

Крім цього, законопроєкт зобов'язує контролера даних — включно із представниками бізнесу — **повідомляти суб'єкта персональних даних у разі їх витоку.** Тут документ пропонує три винятки: контролер вжив достатніх технічних та організаційних заходів захисту, контролер вжив заходів запобігання настання ризиків для прав суб'єкта або ж коли повідомлення становить надмірний тягар для контролера. І хоча самі по собі винятки є досить дискусійними з огляду на всеохопність, запровадження загального правила все ж таки покладатиме нові обов'язки на контролера персональних даних.

Важливим аспектом для контролерів також є **строк розгляду звернень громадян.** Відповідно до статті 27 законопроєкту, суб'єкт може звернутися до

контролера з вимогою реалізувати власні права, передбачені законодавством. Контролер водночас ухвалює рішення невідкладно, але не довше, ніж протягом місяця з дня отримання звернення. Якщо питання стосується **чутливих даних, контролер має 10 днів на розгляд.** Такі звернення можуть стосуватися і відкликання згоди на оброблення даних, і реалізації права на забуття. Отже, компанії матимуть достатній строк на розгляд скарги чи вимоги їхніх клієнтів або споживачів послуг.

Для контролерів, які створені чи працюють за кордоном, законопроєкт пропонує ввести обов'язок призначити свого представника на території України, якщо компанія використовує персональні дані українських користувачів. Умовами реалізації такої вимоги є систематичне оброблення персональних даних з боку компаній, а також наявність одного з таких чинників:

1) контролер обробляє персональні дані громадян України;

2) оброблення персональних даних пов'язане з пропонуванням робіт, послуг чи товарів особам в Україні;

3) оброблення персональних даних пов'язане з моніторингом поведінки суб'єктів на території України.

Крім цього, законопроєкт пропонує значно **збільшити розмір санкцій як для фізичних, так і для юридичних осіб, що порушують законодавство** у сфері захисту персональних даних. Компанії в разі порушення муситимуть сплатити штраф **до 150 мільйонів гривень.** Для порівняння: у GDPR найбільший штраф сягає 20 мільйонів євро (понад 640 мільйонів гривень).

Отже, на приватні компанії очікує суттєва кількість новел процедурного характеру, а також потенційна зміна внутрішніх стандартів і часткова реорганізація роботи з персональними даними користувачів їхніх сервісів.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Результати першого дослідження *Індексу захисту персональних даних* дають підстави для **поміркованого оптимізму щодо стану корпоративної культури приватності та захисту персональних даних у великих технологічних компаніях в Україні** станом на липень 2021 року. **Менш як половина** з 20 компаній (а точніше, 8), що були обрані для дослідження, показали зведені результати **нижче від 50% максимально можливих балів.**

Водночас, з огляду на зростання ролі технологічних компаній за умов швидкого розвитку цифрового простору, **потреба в захисті персональних даних користувачів зростає.** Саме **великі дані** (big data) сьогодні **є найціннішим активом у світі,** де лідерство в приватному секторі отримують ті, хто здатен накопичувати та аналізувати великі масиви даних за допомогою штучного інтелекту та машинного навчання. Серед українських технологічних компаній **вже є лідери, і їхня роль та впливовість** на формування правових відносин, запровадження «правил гри» в онлайн-просторі тільки зростатиме. Ми пропонуємо всім компаніям, обраним для дослідження, **детально ознайомитися з результатами *Індексу захисту персональних даних*, обговорити з командою проєкту пропоновані зміни й оновити свою корпоративну політику конфіденційності та захисту персональних даних.**

- Найкращі результати серед 20 досліджувальних компаній **продемонстрували Olx.ua з показником 77,5%, Ukr.net та Foxtrot.ua з показниками 70% балів кожна** з максимально можливих 100% як відображення стану корпоративної політики приватності та захисту персональних даних користувачів.

- Утім, навіть для Olx.ua, Ukr.net та Foxtrot.ua **є простір для вдосконалення своєї корпоративної політики,** зокрема в аспектах **дотримання принципу мінімізації даних** користувачів, які збираються (Olx.ua), публікації попередніх версій політики конфіденційності на сайтах (Olx.ua, Ukr.net), надання користувачам змоги **отримати копію своїх персональних даних,** зазначення **часових меж відповідей** на запити користувачів (Ukr.net).

- **Щонайменше 50%** максимальної кількості балів отримали **12 із 20 приватних компаній** за критерієм захисту персональних даних. **Корпоративну політику цих компаній оцінюються як середнього та вищого від середнього рівня** в контексті забезпечення дієвого захисту персональних даних своїх клієнтів. До цих компаній увійшли **Kyivstar.ua, Comfy.ua, Allo.ua, Kasta.ua, Prom.ua, NovaPoshta.ua, Vodafone.ua, Zakaz.ua, Citrus.ua та вже згадані Olx.ua, Ukr.net та Foxtrot.ua.**

- Зазначеним компаніям варто звернути увагу на дотримання **принципу мінімізації даних,** які вони збирають про користувачів, **публікування політики конфіденційності в простій та доступній формі** на своєму сайті, чітке прописання у своїй політиці, **способу передавання даних третім особам** тощо.

- **8 із 20 компаній,** обраних для дослідження, набрали **менше ніж 50%** балів з максимально можливих за критерієм захисту персональних даних. Серед них — **Eldorado.ua, DataGroup.ua, Lifecell.ua, Rozetka.com.ua, Makeup.com.ua, Silpo.ua, Lanet.ua та Triolan.com.**

- У більшості із зазначених компаній є значні **недоліки в усіх чотирьох категоріях — від дотримання вимог національного законодавства до зручності користування сайтом та інклюзивності.** Менеджменту цих компаній варто переглянути корпоративну політику приватності та захисту персональних даних, розробити і реалізувати план з посилення політики конфіденційності.

- На сайтах **чотирьох компаній** (Vodafone.ua, Silpo.ua, Triolan.com, Lanet.ua) **немає відмітки для користувача про надання дозволу на оброблення його персональних даних**, хоча це одна з вимог законодавства.

- **10** досліджуваних компаній **не інформують** своїх користувачів, **впродовж якого часу ці компанії зберігатимуть інформацію про користувача.**

- На сайтах **4 компаній** (Triolan.com, Makeup.com.ua, Silpo.ua, Lanet.ua) користувачі **не мають можливості видалити свої збережені особисті дані.**

- **15** досліджуваних компаній **не описують умов видалення акаунту** користувача після припинення договору / за умов некористування акаунтом.

- **10** досліджуваних компаній не вказують, **де та як вони зберігають дані користувачів** (розташування серверів).

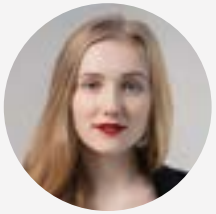
- Якщо згрупувати досліджувані компанії за принципом надання послуг, то серед трьох ключових операторів **Kyivstar.ua та Vodafone.ua набрали відповідно 60% і 52,5% максимальної кількості балів** за критерієм реалізації корпоративної політики приватності та захисту персональних даних. Водночас **Lifecell.ua отримав 45%** максимальної кількості балів (деталі — нижче).

- У категоріях «Технологічні аспекти роботи сайту» і «Зручність користування та інклюзія» Lifecell.ua отримав доволі високі оцінки — 62,5% та 70%. Водночас компанії треба звернути увагу на такі аспекти політики конфіденційності: додати на сайт Lifecell.ua відмітки для користувача про надання дозволу на оброблення його персональних даних, розробити та опублікувати на сайті політику конфіденційності додатково до наявних умов і порядку надання телекомунікаційних послуг обсягом 39 сторінок, надати користувачу змогу отримати копію своїх персональних даних через запит до компанії.

- **Серед групи провайдерів**, що були об'єктом дослідження, **усі компанії отримали оцінки нижчого за середній рівень** за критерієм реалізації корпоративних політик приватності та захисту персональних даних — **DataGroup.ua (47,5%), Lanet.ua (25%) та Triolan.com (15%).** Двом останнім компаніям варто докласти зусиль, щоб з допомогою юристів удосконалити політику конфіденційності та дотримувати її.

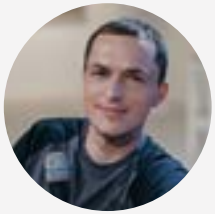
- Ознайомитися з результатами дослідження **кожної з 20 приватних компаній** можна в анкеті **за посиланням *bit.ly/personaldataUA*.**

АВТОРИ ДОСЛІДЖЕННЯ



Тетяна Авдєєва

Юристка з медійного права та менеджерка проєкту зі штучного інтелекту в Центрі демократії та верховенства права (ЦЕДЕМ), а також юристка Незалежної медійної ради. Випускниця Національного університету «Києво-Могилянська академія» зі спеціалізацією в захисті прав людини. Співорганізаторка та суддя міжнародних юридичних змагань з медійного права Price Media Law Moot Court Competition. До сфери професійного інтересу Тетяни належать права людини, міжнародне публічне та міжнародне гуманітарне право, правове регулювання інноваційних технологій та інтернету.



Павло Бєлоусов

Експерт з питань цифрової безпеки ГО «Інтерньюз-Україна», консультант Школи цифрової безпеки DSS380, експерт проєкту TrollessUA. Проводить тренінги із цифрової безпеки для журналістів, що охоплюють теми захисту облікових записів від зовнішніх загроз, конфіскації, втрати інформації, налаштування конфіденційної комунікації в соцмережах, пошуку та розпізнавання так званих FB-тролів.

Аліна Правдиченко

Юристка, спеціалізується в питаннях медійного права та захисту персональних даних. Автор багатьох публікацій на ці теми. Має значний досвід співпраці з неурядовими організаціями та приватним сектором, а також досвід академічної та викладацької діяльності. Випускниця Annenberg-Oxford Media Policy Summer Institute. Членкиня Комітету з медіа та рекламного права НААУ. Юридичну освіту здобула в Донецькому національному університеті ім. В. Стуса.

Лідія Волкова

Юристка, спеціалізується в питаннях прав людини, міжнародного гуманітарного, кримінального та медіаправа. Має досвід співпраці з різними національними та міжнародними організаціями, серед яких ГО «Інтерньюз-Україна», Global Rights Compliance тощо. Юридичну освіту здобула в Національному університеті «Києво-Могилянська академія».

Віталій Мороз

Консультант із цифрових технологій, допомагає організаціям і медіа впроваджувати стратегії та інноваційні підходи в цифровому просторі. Останні роки працював керівником програм нових медіа в ГО «Інтерньюз-Україна», де відповідав за розвиток освітніх та адвокаційних проєктів, зокрема проєктів з адвокації вільного інтернету в Україні та Школи цифрової безпеки DSS380. Здобув освіту в Національному університеті «Києво-Могилянська академія» та в університеті Emerson College у Бостоні за Програмою імені Фулбрайта. Провів понад 500 навчань, виступів на теми цифрових інновацій, медіаграмотності, цифрової безпеки. Автор досліджень у тематиці технологій.